Silverfort

CASE STUDY

How IRCEM strengthened identity security posture to meet compliance requirements and secure privileged accounts

BASED
Lille, France

INDUSTRY
Insurance

USERS
750

ENVIRONMENT
On-prem Active Directory, Windows and Linux servers, VDI, EntraID, Microsoft Authenticator, Yubikey, VMware

IRCEM is a Lille-based social protection organization serving individuals employed in the personal and home care sectors across France. As a member of the Agirc-Arrco network, IRCEM plays a central role in managing retirement and complementary pension benefits for a broad population of domestic workers, caregivers, and service professionals.

THE CHALLENGE:

Meet regulatory requirements and protect privileged accounts

- Comply with government-mandated MFA requirements and secure high-privileged accounts
- Enforce MFA on domain admin accounts across on-prem resources
- Gain visibility into on-prem service accounts activity and legacy authentication attempts

THE SOLUTION:

Complete compliance readiness and real-time protection for privileged accounts

- Met Agirc-Arrco audit requirements and implemented mandated MFA security controls
- Secured all privileged user accounts with MFA across their on-prem environment
- Gained full visibility into on-prem service account activity and legacy authentications

The challenge: Enforcing secure access for privileged accounts under regulatory pressure

With increasing oversight from state-mandated regulatory authorities, IRCEM faced increasing pressure to secure its privileged accounts and comply with mandated identity security controls. Agirc-Arrco, a French state agency that regulates retirement and pension organizations, conducted an audit and made their requirements clear: securing domain admins and service accounts was no longer optional – it was mandatory.

IRCEM recognized this critical gap in their existing identity security layer and understood the need to strengthen security controls for both human and non-human identities (NHIs) without disrupting daily security operations. The ideal solution had to have the ability to enforce MFA for high-privileged users and provide real-time visibility into service accounts' activity. IRCEM sought a solution that could seamlessly integrate into their on-premises environment, without requiring complex configurations or a lengthy deployment process.

Finding the right identity security platform

IRCEM began evaluating solutions to strengthen identity security controls across their on-prem environment. Initially, they explored several traditional PAM solutions to monitor and protect privilege accounts through session control.

"The problem with traditional PAM solutions was that it worked for admin accounts, but they lacked capabilities around securing service accounts. We needed a solution that could protect both privileged users and non-human identities without disrupting our daily operations," said Guillaume Leduc, System IT Administrator at IRCEM

IRCEM needed more granular visibility into service account's authentication trails. After seeing a demo from Silverfort's local partner in France, Wakers, IRCEM was impressed by the platform's capabilities and moved forward with a proof of concept (POC).

> "We needed to understand how our service accounts behaved – what systems they were accessing, where they were authenticating from, and whether any of that activity was risky. Without that visibility, we were operating in the dark. We needed a solution that could detect anomalies, and enforce MFA across our entire environment, including Active Directory."
>
> — Guillaume Leduc, System IT Administrator at IRCEM

The solution: A smooth rollout with immediate visibility and protection

After a successful proof of concept, IRCEM moved quickly to deploy Silverfort across its environment. IRCEM completed the deployment in two weeks with support from Wakers and quickly transitioned to managing the platform independently, ultimately securing 20 sensitive service accounts and 24 highly-privileged users.

> "We use Silverfort to secure access to our critical systems. When we go to the servers, Windows or Linux, or manage VMware or Active Directory, we get prompted for MFA. It's a small change, but it adds a big layer of protection."
>
> — Guillaume Leduc, System IT Administrator at IRCEM

They also integrated Silverfort with Microsoft Teams to receive real-time alerts on security events with different risk levels, helping them with account behavior monitoring and malicious activities in-depth investigation.

"With Teams alerts coming directly from Silverfort, we're not just monitoring – we're able to respond. If something changes in how an account behaves, we see it right away and can act before it escalates," said Leduc

For service accounts, IRCEM leveraged Silverfort's report-only mode to observe authentication patters without disrupting machine-to-machine operations. Once they gained confidence in the expected behavior of each service account, the IT team gradually applied deny policies, using Smart Policy to automate decision-making process and reduce manual overhead.

> "Silverfort is more powerful than our SIEM solutions when it comes to Active Directory. Now, if there's an identity-related issue, my colleagues from other security teams tell me: **Check Silverfort first.**"
>
> — Guillaume Leduc, System IT Administrator at IRCEM

IRCEM started with MFA enforcement for its privileged users and then shifted focus to securing service accounts. The IT team began by monitoring service account activity to understand how each one behaved, prioritizing visibility before enforcements, particularly for accounts used across critical systems. Once IRCEM had a clear baseline, they used Silverfort's Smart Policy to apply conditional access controls and block risky usage without disrupting operations.

Silverfort's logs screen became one of the key capabilities for IRCEM IT team's daily operations, often replacing traditional SIEM tools for identity-related investigations. The team found it easier to identify failed authentications, outdated credentials, and weak protocols usage, including NTLM – all of which were previously challenging to trace.

With Silverfort, IRCEM met strict compliance requirements, secured its privileged accounts, and gained visibility into service account activity – all through a fast, seamless deployment that strengthened its overall identity security posture.

About Silverfort

Silverfort secures every dimension of identity. We deliver end-to-end identity security that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity, analyze exposures, and enforce protection inline to stop lateral movement, ransomware, and other identity threats.

Learn more